

## REMARKS

Claims 1-72 and 101 are pending and stand rejected. Reconsideration is requested. Claims 73-100 have been canceled. Claims 1, 20, 54, 63 and 64 have been amended. Claim 102 has been added. Claims 1-72, 101 and 102 remain in the case for reconsideration.

All pending claims stand rejected as obvious from Bianco et al. U.S. 6,256,737 in view of O'Flaherty US2001/001247A1 and Cavoukian "Building in Privacy" (10 June 1996). Some dependent claims are rejected on the same references further in view of, variously, Herz, Shannon, Stock et al., and Mann et al.

All claims are allowable under 35 U.S.C. Section 103 over the prior art of record for three reasons. First, Bianco et al. is not properly a reference with respect to all claims supported by parent application, Serial No. 09/244,784, now U.S. Pat. No. 6,012,039. Second, none of the references, particularly Bianco et al., teach use of a rule module after authentication or identification of a user, as claimed. Third, with respect to claim 101, the "session key" of Bianco is different from, and used differently from, the "access key" of claim 101, or the "user identification code" of similar but broader claim 102.

### Parent U.S. Pat. No. 6,012,039 predates Bianco et al.

The primary reference, Bianco et al., was filed March 19, 1999. This pending application was filed September 16, 1999, but claims priority from Serial No. 09/244,784, filed February 5, 1999, which is before the earliest effective date of Bianco et al. as a reference under 35 U.S.C. § 102e.

Claim 1 is fully supported in parent application, Serial No. 09/244,784, now U.S. Pat. No. 6,012,039, as follows (all references are to column and line number of the parent '039):

A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

Parent '039, column 3, lines 47-55, describes a method for processing tokenless biometric transactions using an electronic identicator and at least one user (recipient) biometric sample. These transactions involve at least one transmission step. See '039, col. 3, lines 64-67. Communications are further described at '039, col. 8, lines 10-24.

The electronic rule module clearinghouse of claim 1 is called an electronic reward registry in the parent '039 patent. As further discussed below, the described operations of the

registry are those of the more-generally claimed clearinghouse. See '039, col. 4, lines 26-36; and further description at col. 11, line 17, to col. 12, line 10.

(a.) a user registration step, wherein a user registers with an electronic identifier at least one registration biometric sample taken directly from the person of the user;

User registration is described at '039, col. 3, lines 55-58, and further at col. 6, line 67 to col. 7, line 7 and col. 13, lines 52-64.

(b.) formation of a rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user;

The rule module is described at '039, col. 13, lines, 30-46, and its operation is described at col. 11, lines 1-16. The pattern data can include the criteria and conditions at col. 13, lines 32-36, col. 11, line 60 to col. 12, line 2.

(c.) a user identification step, wherein the electronic identifier compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user;

User identification is described at col. 4, lines 1-8 and further at col. 9, line 37 to col. 10, line 33.

(d.) a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the user presenting smartcards or magnetic swipe cards.

Execution upon successful identification is described generally at col. 4, lines 8-13, and further at col. 12, lines 3-25. That this process is conducted tokenlessly--without smartcards or magnetic swipe cards--is described in the '039 Abstract and at col. 4, lines 8-13.

Additionally, it should be noted that pending claim 1 is similar in many respects to '039 method claim 16. Equating it to claim 1, '039 claim 16 includes creating (formation) an electronic registry (rule module clearinghouse) from which reward units are disbursed (an execution command) based on the occurrence of predetermined criteria (pattern data associated with the execution command); registration with an identifier; an identification step in which a

bid biometric sample is compared with a registration biometric sample to produce a successful or failed identification; and a reward issuance step in which the transaction (transmission) is carried out without smart cards or magnetic stripe cards.

Based on the foregoing, it can be seen that the parent of this application disclosed the invention of claim 1 before the effective date of Bianco et al. as a reference under 35 U.S.C. § 102e. Accordingly, Bianco et al. should be removed as a reference under 35 U.S.C. § 103 and claim 1 should be allowed. Claims 2-19, 26-29, 30-38, 52 and 53 depend from claim 1, stand rejected on the same grounds, and should likewise be allowable together with claim 1.

Independent claim 20 is directed to a system which is operative to implement the method of claim 1, couched in substantially similar language and rejected on substantially the same grounds as claim 1. Claim 20 is likewise supported by the disclosure of the '039 patent as discussed above, and further on generally similar '039 device claim 16. Accordingly, Bianco et al. should be removed as a reference under 35 U.S.C. § 103 and claim 20 should likewise be allowable over Bianco et al. in view of O'Flaherty and Cavoukian. Dependent claims 20-24 and 39-51 depend from claim 20 and should likewise be allowable with claim 20.

Independent claim 54 is directed to a method similar to that of claim 1, couched in substantially similar but somewhat broader language, and rejected on the same grounds as claim 1. Claim 54 is supported by the '039 patent in the same manner as claim 1. Accordingly, claim 54 should likewise be allowable over Bianco et al. in view of O'Flaherty and Cavoukian. Dependent claims 55-62 depend from claim 54 and should likewise be allowable with claim 54.

Independent claim 64 is directed to a system which is operative to implement the method of claim 54, couched in substantially similar language and rejected on the same grounds as claim 54. Claim 64 is supported by the '039 patent in the same manner as claim 1. Accordingly, claim 64 should likewise be allowable over Bianco et al. in view of O'Flaherty and Cavoukian. Dependent claims 64-72 depend from claim 64 and should likewise be allowable with claim 64.

Claims 25 and 63 encompass the same subject matter as in claim 1, adding limitations about secondary or subordinated users and secondary or subordinated rules modules. Claim 63 stands rejected on the same grounds as claim 1, and should be allowable together with claim 1.

Claim 25 is separately rejected but the rejection is based on Bianco, too, and the Examiner does not distinguish primary or subordinate users (See Action dated 07/06/2006 at page 11, lines 4-7) and so claim 63 should likewise be allowable.

Furthermore, Bianco does not teach secondary or subordinated users or rule modules as claimed. The Examiner cites Bianco col.2, lines 53-66, but this only contains a general

description of the Bianco system and method, refers to a collection of biometric policies and templates and says nothing about subordination of policies or users. The Examiner also cites col. 18, lines 8-17, referring to FIG. 5, but this text and FIG. 5 merely describe and show groupings at a single level, nothing about subordinated some users or rule modules in relation to other, primary users or modules. The Examiner also cite col. 49, lines 8-65. Again nothing in the cited section, which again references FIG. 5 teaches or suggests any sort of hierarchy in which some users or rule modules are subordinated relative to, or within, or in a tree structure with, other users or rule modules. The biometric groups and other data types shown in FIG. 5 constitute a “one deep” kind of data structure; no subordination or other multi-layer data structure appears to be taught or suggested by Bianco or the other references. Accordingly, Claims 25 and 63 should also be allowable

Claimed Rule Module Is Applied AFTER Authentication or Identification

As previously argued, in all of Applicant’s claims the rule modules are invoked *after* identification or authentication of the user. See, for example, Applicant’s Amendment filed August 4, 2005, at page 28. The biometric policies of Bianco (which the Examiner equates to Applicant’s rule modules) are applied in connection with determining whether a user may access the system. The Examiner has not identified any teaching in Bianco or the other references that teach or suggest a method or system in which rule modules are invoked *after* identification or authentication of the user.

The “access key” of Claim 101 is Patentably Distinct from the “session key” of Bianco.

Claim 101 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application 2001/0011247 to O’Flaherty et al. and “Building in Privacy” by Cavoukian (“Cavoukian”). But the Examiner only cites Bianco in rejecting claim 101, and only mentions Bianco’s session keys from column 51, line 16. The rejection appears to be incomplete, as the Examiner has not indicated where any other features of claim 101 can be found in any of the references.

As stated above, the Examiner cites to the “session keys” of Bianco as teaching the “access key” of claim 101. The Applicant respectfully disagrees. First, the Applicant points

out that Bianco does not explain what a “session key” is in his parlance: the term is not used anywhere else in Bianco. So, the term “session key” needs to be interpreted as would be understood by a person skilled in the art. A “session key” is a key that two parties independently generate, that they can use to secure communications for a single session (*see, e.g.*,

[http://www.google.com/search?hl=en&lr=&defl=en&q=define:Session+key&sa=X&oi=glossary\\_definition&ct=title](http://www.google.com/search?hl=en&lr=&defl=en&q=define:Session+key&sa=X&oi=glossary_definition&ct=title), titled “define:Session key – Google search”, a copy of which is attached hereto). Please note that this understanding is consistent with Bianco, who describes the session keys as being used to encrypt the biometric templates for transmission over the network.

There are two points worth noting about session keys. First, session keys are not transmitted, as such transmission would defeat the purpose of the session key: anyone who could intercept the session key could then decrypt all communications encrypted using the session key. Second, a session key involves just two parties.

In contrast, claim 101 recites “transmitting at least one access key to the terminal” and “receiving a request to validate the at least one access key from the third party Internet location that has received a request from the terminal to access data residing at the third party Internet location”. There are three parties involved in the access key: the first party, which transmitted the access key to the terminal; the terminal, which received the access key from the first party; and the third party Internet location which is requesting validation of the access key. As taught in claim 101, the access key must be transmitted to a terminal and a request to validate the access key must be received from a third party internet location. A session key as commonly understood does not teach either.

Because none of the individual references teach or suggest the above-described features, the combination also cannot teach or suggest these features. Therefore, because none of Bianco, O’Flaherty, or Cavoukian teach an access key, claim 101 is patentable under 35 U.S.C. § 103(a) over Bianco in view of O’Flaherty and Cavoukian.

Accordingly claims 101 and 102 are allowable.

In view of the foregoing amendments and remarks, applicant believes the application should be in condition for allowance. If any questions remain, the Examiner is requested to call the undersigned.

Respectfully submitted,

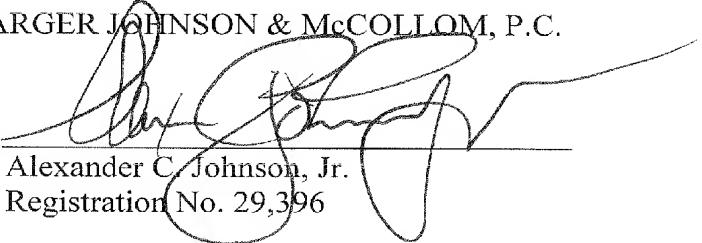
20575

Customer No.

MARGER JOHNSON & McCOLLOM, P.C.

By

Alexander C. Johnson, Jr.  
Registration No. 29,396



210 S.W. Morrison Street, Suite 400  
Portland, Oregon 97204  
Telephone: (503) 222-3613